

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-062803

(43)Date of publication of application : 28.02.2002

(51)Int.Cl.

G09C 1/00
 B42D 11/00
 G06F 17/60
 G06F 19/00
 G06K 19/06
 G07D 7/20

(21)Application number : 2000-252054

(71)Applicant : DAINIPPON PRINTING CO LTD

(22)Date of filing : 23.08.2000

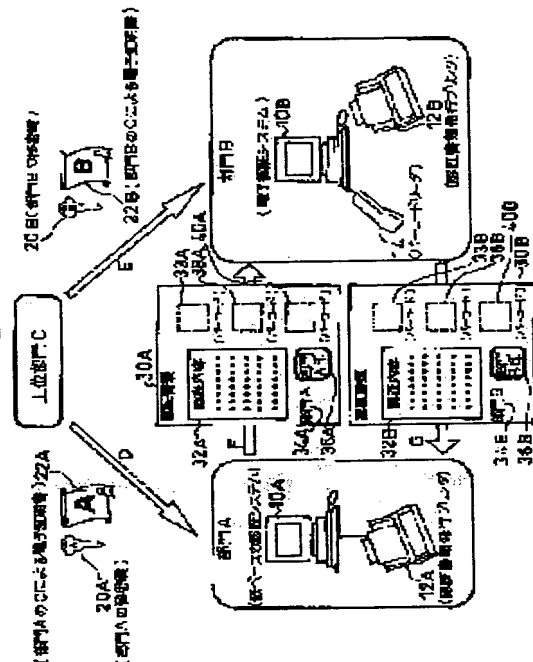
(72)Inventor : MORITA YORIKO

(54) AUTHENTICATION DOCUMENT, AUTHENTICATION FORM, AND SYSTEM FOR ISSUING AND VERIFYING AUTHENTICATION DOCUMENT

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an authentication document applicable to both of an electronic authentication system and a paper-base authentication system.

SOLUTION: Visibly confirmable authentication contents 30A, 30B, authenticator information 34A, 34B, and authenticator's seal imprints 36A, 36B are described in authentication certificates 30A, 30B together with bar codes 33A, 33B of authentication contents data in which the authentication contents 32A, 32B are described, bar codes 38A, 38B of electronic signature data enciphering the authentication contents data, and bar codes 40A, 40B of electronic certificate data of the authenticator.



* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1]Certificates of attestation, wherein both the contents of attestation, authentication person information and an authentication person seal which can be checked by vision, a bar code of the contents data of attestation which described said contents of attestation and a bar code of electronic signature data which enciphered this contents data of attestation, and ** are indicated

[Claim 2]The certificates of attestation according to claim 1, wherein a bar code of electronic certificate data of an authentication person by a certificate authority is further indicated by said certificates of attestation

[Claim 3]The certificates of attestation according to claim 1 or 2, wherein said contents data of attestation is described by a markup language

[Claim 4]The certificates of attestation according to any one of claims 1 to 3 which said electronic signature data hash-izes said contents data of attestation, and are characterized by being the data enciphered with an authentication person's secret key

[Claim 5]The certificates of attestation according to any one of claims 1 to 4, wherein said bar code is a two-dimensional bar code

[Claim 6]The certificates of attestation according to any one of claims 1 to 4 bar-code-izing after changing into text data when-izing of said data cannot be carried out [a direct bar code]

[Claim 7]The certificates of attestation according to claim 2, wherein said electronic certificate data is an authentication person's public key and a signature algorithm which were attested by certificate authority

[Claim 8]Authentication person information, an authentication person seal, and an attestation paper, wherein an authentication person's electronic certificate data is printed beforehand.

[Claim 9]An issuing method of certificates of attestation characterized by comprising the following.

A procedure of calling the contents data of attestation which described the contents of attestation from a database.

A procedure which enciphers data which described said contents of attestation, and creates electronic signature data.

A procedure which bar-code-izes each data.

A procedure which prints a bar code of the contents data of attestation which described the contents of attestation which can be checked by vision, authentication person information and an authentication person seal, and said contents of attestation, and a bar code of electronic signature data which enciphered this contents data of attestation.

[Claim 10]An issuing method of the certificates of attestation according to claim 9 characterized by comprising the following.

A procedure of calling electronic certificate data of an authentication person by a certificate authority.

A procedure which bar-code-izes this electronic certificate data, and a procedure which prints this bar code.

[Claim 11]An issuing method of the certificates of attestation according to claim 9 or 10 including a procedure which markup-language-izes said contents data of attestation.

[Claim 12]An issuing method of the certificates of attestation according to any one of claims 9 to 11 including a procedure of changing into text data data which cannot carry out [a direct bar code]-izing.

[Claim 13]An issuing method of the certificates of attestation according to any one of claims 9 to 12 creating said electronic signature data by hash-izing said contents data of attestation, and enciphering with an authentication person's secret key.

[Claim 14]An issuing device of certificates of attestation characterized by comprising the following.

A means to call the contents data of attestation which described the contents of attestation from a database.

A means to encipher data which described said contents of attestation, and to create electronic signature data.

A means to bar-code-ize each data.

A means to print a bar code of the contents data of attestation which described the contents of attestation which can be checked by vision, authentication person information and an authentication person seal, and said contents of attestation, and a bar code of electronic signature data which enciphered this contents data of attestation.

[Claim 15]An issuing device of certificates of attestation characterized by comprising the following.

A means to call the contents data of attestation which described the contents of attestation from a database.

A means to encipher data which described said contents of attestation, and to create electronic signature data.

A means to call electronic certificate data of an authentication person by a certificate authority.

A means to print a bar code of the contents data of attestation which described the contents of attestation which can be checked by vision, authentication person information and an authentication person seal, and said contents of attestation to be means to bar-code-ize each data, a bar code of electronic signature data which enciphered this contents data of attestation, and a bar code of said electronic certificate data.

[Claim 16]A verification method of certificates of attestation characterized by comprising the following.

A procedure of reading a bar code in the certificates of attestation by which both a bar code of the contents data of attestation which described the contents of attestation which can be checked by vision, authentication person information and an authentication person seal, and said contents of attestation, and a bar code of electronic signature data which enciphered this contents data of attestation were printed.

A procedure which decrypts read electronic signature data, and a procedure of comparing what hash-ized this decrypted electronic signature data and said contents data of attestation, and judging this human nature of existence of an alteration, and an authentication person.

[Claim 17]A verification method of the certificates of attestation according to claim 16 including a procedure of reading a bar code of electronic certificate data of an authentication person by a certificate authority currently printed by said certificates of attestation.

[Claim 18]A verification method of the certificates of attestation according to claim 16 including a procedure of calling electronic certificate data of an authentication person by a certificate authority which has come to hand a priori.

[Claim 19]A verification method of the certificates of attestation according to claim 17 or 18 characterized by carrying out decoding of said electronic signature data using an authentication person's public key contained in said electronic certificate data.

[Claim 20]A verification device of certificates of attestation characterized by comprising the following.

The contents of attestation which can be checked by vision, authentication person information and an authentication person seal, a bar code of the contents data of attestation which described said contents of attestation, A means to read a bar code in the certificates of attestation by which both a bar code of electronic signature data which enciphered this contents data of attestation, and a bar code of electronic certificate data of an authentication person by a certificate authority were printed.

A means to decrypt read electronic signature data, and a means to compare what hash-ized this decrypted electronic signature data and said contents data of attestation, and to judge this human nature of existence of an alteration, and an authentication person.

[Claim 21]A verification device of certificates of attestation characterized by comprising the following.

A means to read a bar code in the certificates of attestation by which both a bar code of the contents data of attestation which described the contents of attestation which can be checked by vision, authentication person information and an authentication person seal, and said contents of attestation, and a bar code of electronic signature data which enciphered this contents data of attestation were printed.

A means to call electronic certificate data of an authentication person by a certificate authority which has come to hand a priori.

A means to decrypt read electronic signature data.

A means to compare what hash-ized decrypted this electronic signature data and said contents data of attestation, and to judge this human nature of existence of an alteration, and an authentication person.

[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention relates to certificates of attestation, an attestation paper, and issue and the verification system of certificates of attestation, The certificate issuing and registration processings especially in public institutions, such as a government office, such as a resident card and a certified seal registration, Either the suitable electronic authorization system using a digital signature to use for uses, such as general receipt issue and accounting, or the authentication system of the conventional paper basis is related with issue and/or verification method, and device of available certificates of attestation, the attestation paper for it, and certificates of attestation.

[0002]

[Description of the Prior Art]To the conventional certificates of attestation, for example, the resident card, and certified seal registration of paper, the authentication person seals (for example, mayor seal) etc. are indicated to be the contents of attestation (address and name or seal), and authentication person information (for example, government office name). When publishing these certificates of attestation in large quantities, the contents and a seal are printed with a printer by the attestation paper which performed processing which the duplicate of a copy etc. tends to distinguish. On the other hand, when a receiver checks certificates of attestation, thing of the certificates of attestation of paper is not forged, or a receiver judges visually.

[0003]The electronic authorization system using public key infrastructure (Public Key Infrastructure:PKI) which recent years, for example, an applicant, proposed by JP,10-135943,A is spreading. An authentication person's electronic signature data to the contents data of attestation and this contents data of attestation which described the contents of attestation in order to realize attestation within this system (as the applicant proposed by JP,2000-4222,A) The data which hash-ized the contents data of attestation, for example, and was enciphered with the authentication person's secret key and an authentication person's electronic certificate data (an authentication person's public key, a signature algorithm, etc. which were attested by the certificate authority of the higher rank), and the electronic certificate of a certificate authority are required.

[0004]Although it is thought that the certificates of attestation of the conventional paper change to electronic data with the spread of electronic authorization systems, A simultaneous change is more difficult, as an employment scale is large since a large system change and system equipment introduction are needed in order to change from the authentication system of the certificates-of-attestation base (a paper basis is only called hereafter) of paper to an electronic authorization system. Therefore, the operation system with which it was rare when all the authentication systems changed at once, and the authentication system of a paper basis and the electronic authorization system lived together for a while is taken in many cases. In that case, the situation of performing the office procedure in the section which is performing the electronic authorization system based on the certificates of attestation of the paper of the section which is applying by the authentication system of the paper basis occurs. There is the necessity of electronic-data-izing the certificates of attestation of paper under such a situation. On the

contrary, the situation of performing the office procedure in the section which is performing attestation in a paper basis based on the electronic data of the section which is applying by the electronic authorization system occurs. It is necessary to use electronic data as the certificates of attestation of paper under such a situation.

[0005]In order to treat the certificates of attestation of paper as electronic data by the conventional method, the following methods are generally considered.

[0006](1) Incorporate the certificates of attestation of paper as a picture with a scanner, and save image data.

[0007](2) Carry out a punch input and electronic-data-ize the contents of the certificates of attestation of paper.

[0008](3) By OCR (optical character reader), carry out character recognition and electronic-data-ize the certificates of attestation of paper.

[0009]

[Problem(s) to be Solved by the Invention]However, the above-mentioned method had the following problems, respectively.

[0010]In the method of (1), although the picture of the certificates of attestation of paper can be saved, since it is not directly electronized about the content sentences (text) in it, secondary practical use of the content sentences of certificates of attestation cannot be performed.

[0011]In order that human being may read the content sentences of certificates of attestation visually and may do a punch input, the method of (2) takes a help and there is possibility of an erroneous input by it.

[0012]Although machinery reading is carried out in the method of (3), if all of a gestalt, an entry place, etc. of certificates of attestation are not the same certificates of attestation, it is difficult to read. For example, since a size, a place, etc. of a character which are described for every local self-governing body are various, in such a case, the resident card of local self-governing body issue is not practical.

[0013]As what checks the seal as attestation, and the truth or falsehood of a signature image, to JP,2000-148742,A. Near a seal or the signature image, write the management number and a use number in addition by bar code form, and. The electronic text data storage system which writes the management number of a document, and the code of a storage organization in addition by bar code form into a printing document, and keeps an electronic filing document for realization of an authentication management system and an attestation controlling method, Keeping and managing the management number and text management number of authentication data mutually is indicated by the authentication data storage system which keeps image data, such as a seal of an individual or a legal entity, and a sign, as authentication data.

[0014]According to this method, although it becomes easy [the check of the truth or falsehood of a seal or a signature image], since the contents of the document are not bar-code-ized, the too above problems are produced on the occasion of electronic-data-izing of the contents of a document.

[0015]To Patent Publication Heisei 9-512114, carrying out an image scan, carrying out compression encoding of the whole former document, bar-code-izing it, and attesting it is indicated in the document transmission in a facsimile.

[0016]However, this method can be used only by the exchange of facsimiles with a special function. In order to exchange the raster data in which this document carried out the image scan as it is, when it did not text-data-ize by a certain method, it had a problem of being unable to use the secondary contents of the text.

[0017]Let it be the 1st technical problem for this invention to provide certificates of attestation also with high alteration prevention performance easily [were made in order to cancel said conventional problem, and it is available at both the authentication system of a paper basis, and an electronic authorization system, and / electronic-data-izing].

[0018]This invention makes it the 2nd technical problem to provide an attestation paper suitable for creation of said certificates of attestation again.

[0019]This invention makes it the 3rd technical problem to provide the issuing method and device of said certificates of attestation again.

[0020]This invention makes it the 4th technical problem to provide the verification method and device of said certificates of attestation again.

[0021]

[Means for Solving the Problem]The contents of attestation, authentication person information, and an authentication person seal which can check this invention by vision to certificates of attestation, Said 1st technical problem is solved by indicating both a bar code of the contents data of attestation which described said contents of attestation, and a bar code of electronic signature data which enciphered this contents data of attestation.

[0022]A bar code of electronic certificate data of an authentication person by a certificate authority is also written in said certificates of attestation.

[0023]Said contents data of attestation is described by a markup language.

[0024]Said contents data of attestation is hash-ized, and let said electronic signature data be the data enciphered with an authentication person's secret key.

[0025]Let said bar code be a two-dimensional bar code.

[0026]When-izing of said data cannot be carried out [a direct bar code], after changing into text data, it bar-code-izes.

[0027]Let said electronic certificate data be an authentication person's public key and a signature algorithm which were attested by certificate authority.

[0028]This invention solves said 2nd technical problem again by printing beforehand authentication person information, an authentication person seal, and an authentication person's electronic certificate data on an attestation paper.

[0029]This invention A procedure of calling the contents data of attestation which described the contents of attestation from a database, A procedure which enciphers data which described said contents of attestation, and creates electronic signature data, A procedure which bar-code-izes each data, and the contents of attestation which can be checked by vision, By a procedure which prints a bar code of the contents data of attestation which described authentication person information and an authentication person seal, and said contents of attestation, and a bar code of electronic signature data which enciphered this contents data of attestation, as certificates of attestation are published, said 3rd technical problem is solved.

[0030]It is made to include a procedure of calling electronic certificate data of an authentication person by a certificate authority, a procedure which bar-code-izes this electronic certificate data, and a procedure which prints this bar code.

[0031]It is made to include a procedure which markup-language-izes said contents data of attestation.

[0032]It is made to include a procedure of changing into text data data which cannot carry out [a direct bar code]-izing.

[0033]Said electronic signature data is created by hash-izing said contents data of attestation, and enciphering with an authentication person's secret key.

[0034]This invention A means to call the contents data of attestation which described the contents of attestation for an issuing device of certificates of attestation from a database, A means to encipher data which described said contents of attestation, and to create electronic signature data, A means to bar-code-ize each data, and the contents of attestation which can be checked by vision, Said 3rd technical problem is solved by constituting using a means to print a bar code of the contents data of attestation which described authentication person information and an authentication person seal, and said contents of attestation, and a bar code of electronic signature data which enciphered this contents data of attestation.

[0035]This invention A means to call the contents data of attestation which described the contents of attestation for an issuing device of certificates of attestation from a database, A means to encipher data which described said contents of attestation, and to create electronic signature data, A means to call electronic certificate data of an authentication person by a certificate authority, and a means to bar-code-ize each data, The contents of attestation which can be checked by vision, authentication person information and an authentication person seal, a bar code of the contents data of attestation which described said contents of attestation, Said 3rd technical problem is solved by constituting using a means to print a bar code of electronic

signature data which enciphered this contents data of attestation, and a bar code of said electronic certificate data.

[0036]This invention The contents of attestation, authentication person information, and an authentication person seal which can be checked by vision, A procedure of reading a bar code in the certificates of attestation by which both a bar code of the contents data of attestation which described said contents of attestation, and a bar code of electronic signature data which enciphered this contents data of attestation were printed, By procedure which decrypts read electronic signature data, and a procedure of comparing what hash-ized this decrypted electronic signature data and said contents data of attestation, and judging this human nature of existence of an alteration, and an authentication person, as certificates of attestation are verified, said 4th technical problem is solved.

[0037]It is made to include a procedure of reading a bar code of electronic certificate data of an authentication person by a certificate authority currently printed by said certificates of attestation.

[0038]Or it is made to include a procedure of calling electronic certificate data of an authentication person by a certificate authority which has come to hand a priori.

[0039]It is made to carry out decoding of said electronic signature data using an authentication person's public key contained in said electronic certificate data.

[0040]This invention again a verification device of certificates of attestation The contents of attestation which can be checked by vision, Authentication person information and an authentication person seal, a bar code of the contents data of attestation which described said contents of attestation, A means to read a bar code in the certificates of attestation by which both a bar code of electronic signature data which enciphered this contents data of attestation, and a bar code of electronic certificate data of an authentication person by a certificate authority were printed, Said 4th technical problem is solved by comparing a means to decrypt read electronic signature data with a thing which hash-ized this decrypted electronic signature data and said contents data of attestation, and constituting using a means to judge existence of an alteration.

[0041]This invention again a verification device of certificates of attestation The contents of attestation which can be checked by vision, A means to read a bar code in the certificates of attestation by which both a bar code of the contents data of attestation which described authentication person information and an authentication person seal, and said contents of attestation, and a bar code of electronic signature data which enciphered this contents data of attestation were printed, A means to call electronic certificate data of an authentication person by a certificate authority which has come to hand a priori, Said 4th technical problem is solved by constituting using a means to decrypt read electronic signature data, and a means to compare what hash-ized this decrypted electronic signature data and said contents data of attestation, and to judge existence of an alteration, and this human nature of an authentication person.

[0042]

[Embodiment of the Invention]With reference to drawings, the embodiment of this invention is described in detail below.

[0043]The section A which is applying by the authentication system of a paper basis now as shown in drawing 1. Electronic authentication of the section B, the section A, and the section B which are applying by the electronic authorization system is carried out, for example, the higher rank (management) section C (certificate authority) which is the route certificate authority or the reliable middle certificate authority located in the top is assumed.

[0044]Said section A is equipped with the personal computer 10A containing the database of the contents of attestation, and the printer 12A for certificates-of-attestation issue, for example. As shown to this section A at the arrow D, the secret key data 20A of the higher rank section C to the section A concerned, It is assumed that the electronic certificate data 22A of the section A in which the electronic signature of the higher rank section C is carried out, and the electronic certificate data (graphic display abbreviation) of the section C containing the public key of the higher rank section C are distributed including the public key of the section A concerned.

[0045] Said section B is equipped with the same personal computer 10B and printer 12B as the section A, and the bar code reader 14, for example. As shown to this section B at the arrow E, the secret key data 20B of the higher rank section C to the section B concerned, It is assumed that the electronic certificate data 22B of the section B in which the electronic signature of the higher rank section C is carried out, and the electronic certificate data (graphic display abbreviation) of the section C containing the public key of the higher rank section C are distributed including the public key of the section B concerned.

[0046] First, as shown in the arrow F, the case where paperwork of the certificates of attestation 30A published in the section A of the authentication system of a paper basis is carried out in the section B of an electronic authorization system is explained.

[0047] The procedure of publishing the certificates of attestation 30A in the section A is shown in drawing 2.

[0048] Describe the data which called and called the contents 32A of attestation from the database at Step 100 in the section A according to the request of the issue requesting person of certificates of attestation by markup languages, such as XML, if needed, and. On the specification of a bar code, the binary data which cannot carry out [a direct bar code]-izing is changed into text data, for example by Base64, and let it be the contents data of attestation.

[0049] Subsequently, at Step 102, this contents data of attestation is hash-ized, for example, a message digest is created, it enciphers with the secret key data 20A of the section A, and electronic signature data is created.

[0050] Subsequently, at Step 104, the electronic certificate data 22A by the higher rank section C of the section A is called if needed. When the section A and the section B exchange certificates of attestation frequently, and the section A and the section B exchange a priori the electronic certificate data of the section A and the section B attested by the higher rank section C, the electronic certificate data of certificates of attestation can also be omitted. In this case, Step 104 is unnecessary.

[0051] subsequently, the steps 106, 108, and 110 -- the above -- the data created at Steps 100, 102, and 104 -- respectively -- for example, it two-dimensional-bar-code-izes. It is arbitrary, and when the electronic certificate data of certificates of attestation is omitted especially, naturally Step 110 of the bar-code-ized turn is also unnecessary.

[0052] Subsequently, the contents 32A of attestation (here text) indicated by the certificates of attestation of the conventional paper as it progressed to Step 112 and the numerals 30A showed to drawing 1. In addition to the name 34A of the section A, and the seal 36A of the section A, the bar code 33A of the contents 32A of attestation, the bar code 38A of the electronic signature data created at Step 102, and the bar code 40A of the electronic certificate data created at Step 104 are printed, and it is made the certificates of attestation 30A of paper.

[0053] Next, the certificates of attestation 30A of the paper created as mentioned above are verified by the section B according to a procedure as shown in drawing 3.

[0054] That is, in the section B, the bar code 33A (the contents of attestation), the bar code 38A (electronic signature data), and the bar code 40A (electronic certificate) are first read in the certificates of attestation 30A of paper at Steps 200, 202, and 204, for example using the bar code reader 14 (a scanner may be used). Under the present circumstances, the binary data changed into the text data by Base64 is transformed inversely by Base64, and is returned to binary data. When the bar code of electronic certificate data is omitted, the electronic certificate data which has come to hand a priori is called at Step 204.

[0055] Subsequently, if it checks that the electronic certificate data 22A of the section A described by the bar code 40A, for example is attested in the higher rank section C based on the electronic certificate data of the section C at Step 206, the public key data of the section A contained in this electronic certificate data 22A will be taken out.

[0056] Subsequently, it progresses to Step 208, the electronic signature data read at Step 202 is decrypted using the public key taken out at Step 206, and the message digest i is created.

[0057] Subsequently, it progresses to Step 210, the contents data of attestation read at Step 200 is hash-ized, and the message digest ii is created.

[0058] subsequently -- the case where progress to Step 212, compare the message digests i and

ii, and it is in agreement -- Step 214 -- the person himself/herself of the contents of attestation -- it checks attestation and un-altering.

[0059]progressing to Step 216 on the other hand, when the message digests i and ii are inharmonious -- the person himself/herself of the contents of attestation -- it does not recognize attestation and un-altering.

[0060]Thus, after being able to realize electronization of the contents of certificates of attestation, non-altering proof of the contents of attestation, and principal certification of the section A of certificates of attestation and checking the contents, it becomes possible to treat electronic data by an electronic authorization system promptly.

[0061]On the other hand, as shown in the arrow G of drawing 1, in carrying out paperwork of the documents attested in the section B of the electronic authorization system in the section A of attestation of a paper basis, Like the case of the section A, the contents 32B of attestation conventional also in the section B, the name 34B of the section B, On the seal 36B of the section B, in addition, the contents data of attestation which described the contents of attestation by the markup language, the electronic signature data which hash-ized this and was enciphered with the secret key of the section B, and the electronic certificate data of the section B currently proved by the higher rank section C -- respectively -- for example, the two-dimensional bar codes 33B and 38B -- 40B is formed and it prints as the certificates of attestation 30B of paper. Under the present circumstances, it is binary data, and on the specification of a bar code, when-izing cannot be carried out [a direct bar code], after changing into text data, for example by Base64, it bar-code-izes.

[0062]Since it is a paper basis in the section A in these certificates of attestation 30B, the contents are visually checked as usual with the contents 32B of attestation, the section name 34B, and the section seal 36B. It is a certain fault, and when certificates of attestation need to be returned to the section B from the section A, in the section B, it is possible to read a bar code by the bar code reader 14, and to incorporate the contents again.

[0063]In this embodiment, since the two-dimensional bar code is used as a bar code, it is little area and many information can be described. The kind of bar code is not limited to this.

[0064]In this embodiment, since it is [bar-code-] made toize on the specification of a bar code after changing into text data by Base64 when-izing cannot be carried out [a direct bar code], even if it is binary data, bar-code-izing is possible. It is also possible to use a method called BinHex which the method which changes binary data into text data is not limited to Base64, for example, is used by standard uuencode for UNIX (registered trademark) and Macintosh.

[0065]In this embodiment, since it has bar-code-ized after using the data of markup language XML, an item and the contents become clear and secondary use of the contents of attestation is easy. It is also possible for the kind of markup language not to be limited to XML, but to use HTML, TEX, SGML, etc. It is also possible to omit markup language-ization.

[0066]In said embodiment, although he was trying to print all the information with a printer, For example, as shown in drawing 4, the data in which the bar code 40 grade of the authentication person information 34, the authentication person seal 36, and an authentication person's electronic certificate data was fixed is able to reduce the load of printing using the attestation paper 50 currently printed beforehand.

[0067]The applied object of this invention is not limited to the certificate issuing or registration processing in a local self-governing body, but it is clear general receipt issue and that its it can use for accounting etc. similarly.

[0068]

[Effect of the Invention]According to this invention, electronization of the contents of certificates of attestation, non-altering proof of certificates of attestation, and principal certification of the authentication person of certificates of attestation can be realized, and either the authentication system of a paper basis or an electronic authorization system has the outstanding effect of being available.

[Translation done.]

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-62803

(P2002-62803A)

(43) 公開日 平成14年2月28日 (2002.2.28)

(51) Int.Cl. ⁷	識別記号	FI	テーマコード* (参考)
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 Z 3 E 0 4 1
			6 4 0 B 5 B 0 3 5
B 4 2 D 11/00		B 4 2 D 11/00	U 5 J 1 0 4
G 0 6 F 17/60	1 4 0	G 0 6 F 17/60	1 4 0
19/00	3 0 0	19/00	3 0 0 N

審査請求 未請求 請求項の数21 O L (全 9 頁) 最終頁に続く

(21) 出願番号 特願2000-252054(P2000-252054)

(22) 出願日 平成12年8月23日 (2000.8.23)

(71) 出願人 000002897

大日本印刷株式会社

東京都新宿区市谷加賀町一丁目1番1号

(72) 発明者 森田 より子

東京都新宿区市谷加賀町一丁目1番1号

大日本印刷株式会社内

(74) 代理人 100080458

弁理士 高矢 諭 (外2名)

Fターム(参考) 3E041 AA10 BA15

5B035 AA15 BB01 BC00

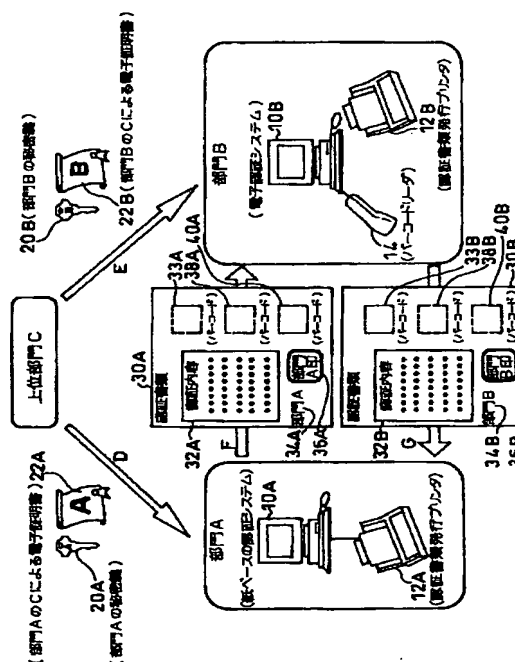
5J104 AA09 LA03 LA06 NA02 PA13

(54) 【発明の名称】 認証書類、認証用紙、及び、認証書類の発行・検証システム

(57) 【要約】

【課題】 電子認証システムと紙ベースの認証システムのどちらでも利用可能な認証書類を提供する。

【解決手段】 認証書類30A、30Bに、視覚により確認可能な認証内容32A、32B、認証者情報34A、34B及び認証者印影36A、36Bと、前記認証内容32A、32Bを記述した認証内容データのバーコード33A、33B、該認証内容データを暗号化した電子署名データのバーコード38A、38B、認証者の電子証明書データのバーコード40A、40Bと共に記載する。



【特許請求の範囲】

【請求項1】視覚により確認可能な認証内容、認証者情報及び認証者印影と、前記認証内容を記述した認証内容データのバーコード、及び、該認証内容データを暗号化した電子署名データのバーコードと、

が共に記載されていることを特徴とする認証書類。

【請求項2】前記認証書類に、更に、認証機関による認証者の電子証明書データのバーコードが記載されていることを特徴とする、請求項1に記載の認証書類。

【請求項3】前記認証内容データが、マークアップ言語で記述されていることを特徴とする、請求項1又は2に記載の認証書類。

【請求項4】前記電子署名データが、前記認証内容データをハッシュ化し、認証者の秘密鍵で暗号化したデータであることを特徴とする、請求項1乃至3のいずれかに記載の認証書類。

【請求項5】前記バーコードが、2次元バーコードであることを特徴とする、請求項1乃至4のいずれかに記載の認証書類。

【請求項6】前記データが、直接バーコード化できない場合、テキストデータに変換してからバーコード化されていることを特徴とする、請求項1乃至4のいずれかに記載の認証書類。

【請求項7】前記電子証明書データが、認証機関によって認証された、認証者の公開鍵や署名アルゴリズムであることを特徴とする、請求項2に記載の認証書類。

【請求項8】認証者情報や認証者印影、及び、認証者の電子証明書データが予め印刷されていることを特徴とする認証用紙。

【請求項9】データベースから認証内容を記述した認証内容データ呼び出す手順と、前記認証内容を記述したデータを暗号化して電子署名データを作成する手順と、

各データをバーコード化する手順と、

視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、及び、該認証内容データを暗号化した電子署名データのバーコードを印刷する手順と、

を含むことを特徴とする認証書類の発行方法。

【請求項10】更に、認証機関による認証者の電子証明書データ呼び出す手順と、

該電子証明書データをバーコード化する手順と、

該バーコードを印刷する手順と、

を含むことを特徴とする、請求項9に記載の認証書類の発行方法。

【請求項11】更に、前記認証内容データをマークアップ言語化する手順を含むことを特徴とする、請求項9又は10に記載の認証書類の発行方法。

【請求項12】更に、直接バーコード化できないデータ

を、テキストデータに変換する手順を含むことを特徴とする、請求項9乃至11のいずれかに記載の認証書類の発行方法。

【請求項13】前記認証内容データをハッシュ化し、認証者の秘密鍵で暗号化することにより、前記電子署名データを作成することを特徴とする、請求項9乃至12のいずれかに記載の認証書類の発行方法。

【請求項14】データベースから認証内容を記述した認証内容データ呼び出す手段と、

10 前記認証内容を記述したデータを暗号化して電子署名データを作成する手段と、

各データをバーコード化する手段と、

視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、及び、該認証内容データを暗号化した電子署名データのバーコードを印刷する手段と、

を含むことを特徴とする認証書類の発行装置。

【請求項15】データベースから認証内容を記述した認証内容データ呼び出す手段と、

20 前記認証内容を記述したデータを暗号化して電子署名データを作成する手段と、

認証機関による認証者の電子証明書データ呼び出す手段と、

各データをバーコード化する手段と、

視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、該認証内容データを暗号化した電子署名データのバーコード、及び、前記電子証明書データのバーコードを印刷する手段と、

30 を含むことを特徴とする認証書類の発行装置。

【請求項16】視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、及び、該認証内容データを暗号化した電子署名データのバーコードが共に印刷された認証書類から、バーコードを読み取る手順と、

読み取った電子署名データを復号化する手順と、

該復号化した電子署名データと前記認証内容データをハッシュ化したものを比較して、改ざんの有無と認証者の本人性を判定する手順と、

40 を含むことを特徴とする認証書類の検証方法。

【請求項17】更に、前記認証書類に印刷されている、認証機関による認証者の電子証明書データのバーコードを読み取る手順を含むことを特徴とする、請求項16に記載の認証書類の検証方法。

【請求項18】更に、事前に入手している、認証機関による認証者の電子証明書データ呼び出す手順を含むことを特徴とする、請求項16に記載の認証書類の検証方法。

50 【請求項19】前記電子証明書データに含まれる認証者の公開鍵を用いて、前記電子署名データを復号化すると

とを特徴とする、請求項17又は18に記載の認証書類の検証方法。

【請求項20】視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、該認証内容データを暗号化した電子署名データのバーコード、及び、認証機関による認証者の電子証明書データのバーコードが共に印刷された認証書類から、バーコードを読み取る手段と、読み取った電子署名データを復号化する手段と、該復号化した電子署名データと前記認証内容データをハッシュ化したものを比較して、改ざんの有無と認証者の本人性を判定する手段と、を含むことを特徴とする認証書類の検証装置。

【請求項21】視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、及び、該認証内容データを暗号化した電子署名データのバーコードが共に印刷された認証書類から、バーコードを読み取る手段と、事前に入手している、認証機関による認証者の電子証明書データを呼び出す手段と、読み取った電子署名データを復号化する手段と、該復号化した電子署名データと前記認証内容データをハッシュ化したものを比較して、改ざんの有無と認証者の本人性を判定する手段と、を含むことを特徴とする、認証書類の検証装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、認証書類、認証用紙、認証書類の発行・検証システムに係り、特に、役所等の公的機関における住民票や印鑑証明等の証明書発行・登録処理、一般の領収書発行、会計処理等の用途に用いるのに好適な、デジタル署名を用いる電子認証システムと従来の紙ベースの認証システムのどちらでも利用可能な、認証書類、そのための認証用紙、認証書類の発行及び／又は検証方法及び装置に関する。

【0002】

【従来の技術】従来の紙の認証書類、例えば住民票や印鑑証明には、認証内容（住所氏名あるいは印影）と、認証者情報（例えば役所名）と、認証者印影（例えば市長印）等が記載されている。この認証書類を大量に発行するような場合は、コピー等の複製が判別し易い加工を施した認証用紙に、プリンタで内容と印影が印刷される。一方、認証書類を受領者が確認する場合は、紙の認証書類の実物が偽造されていないか、受領者が目視で判断する。

【0003】又、近年、例えば出願人が特開平10-135943で提案したような、公開鍵暗号基盤（Public Key Infrastructure: PKI）を利用した電子認証システムが普及してきている。このシステム内で認証を

タ、該認証内容データに対する認証者の電子署名データ（特開2000-4222で出願人が提案したように、認証内容データを例えばハッシュ化し、認証者の秘密鍵で暗号化したデータ）、及び、認証者の電子証明書データ（上位の認証機関によって認証された認証者の公開鍵や署名アルゴリズム等）、認証機関の電子証明書が必要である。

【0004】従来の紙の認証書類は、電子認証システムの普及と共に、電子データに切り替わっていきと考えられるが、紙の認証書類ベース（以下、単に紙ベースと称する）の認証システムから電子認証システムに切り替えるには、大幅なシステム変更や、システム器材導入が必要になるため、運用規模が大きければ大きいほど、一斉切替えが困難である。従って、全ての認証システムが一度に切り替わる場合は稀で、しばらくは、紙ベースの認証システムと、電子認証システムが共存した運用方式が採られることが多い。その際、紙ベースの認証システムで運用を行っている部門の紙の認証書類を元に、電子認証システムを行っている部門での事務手続を行う状況が発生する。そのような状況下では、紙の認証書類を電子データ化する必要性がある。逆に、電子認証システムで運用を行っている部門の電子データを元に、紙ベースでの認証を行っている部門での事務手続を行う状況が発生する。このような状況下では、電子データを紙の認証書類にする必要がある。

【0005】従来の方法で紙の認証書類を電子データとして扱うには、次のような方法が一般的に考えられる。

【0006】（1）紙の認証書類をスキャナで画像として取り込み、画像データを保存する。

【0007】（2）紙の認証書類の内容をパンチ入力して電子データ化する。

【0008】（3）紙の認証書類をOCR（光学的文字読取装置）で文字認識をして、電子データ化する。

【0009】

【発明が解決しようとする課題】しかしながら、上記の方法は、それぞれ、次のような問題点を有していた。

【0010】（1）の方法では、紙の認証書類の画像を保存可能であるが、その中の内容文（テキスト）については直接電子化されないため、認証書類の内容文の2次活用ができない。

【0011】（2）の方法では、人間が認証書類の内容文を目視で読み取り、パンチ入力するため、人手を要してしまい、且つ、誤入力の可能性がある。

【0012】（3）の方法では、機械読取りするが、認証書類の形態や記入場所等が全て同一の認証書類でないと、読み取ることが困難である。例えば地方自治体発行の住民票は、各地方自治体毎に、記述されている文字の大きさや場所等がまちまちであるため、このような場合には、実用的でない。

【0013】なお、認証としての印章やサインイメージ

の真贋の確認を行うものとして、特開2000-148742には、印章やサインイメージの近傍に、その管理番号及び使用番号をバーコード形式で付記すると共に、印字文書の中に、文書の管理番号及び保管機関のコードをバーコード形式で付記し、認証管理システム、及び、認証管理方法の実現のため電子文書を保管する電子文章データ保管システムと、個人や法人の印章やサイン等のイメージデータを認証データとして保管する認証データ保管システムで、相互に認証データの管理番号と文章管理番号を保管及び管理することが記載されている。

【0014】この方法によれば、印章やサインイメージの真贋の確認は容易となるが、文書の内容はバーコード化されていないので、文書内容の電子データ化に際しては、やはり前記のような問題点を生じる。

【0015】又、特表平9-512114には、ファクシミリでの文書送信において、元文書全体を画像スキャンし、圧縮・符号化し、バーコード化して認証することが記載されている。

【0016】しかしながら、この方法は、特殊機能を持つファクシミリ同士のやりとりでしか利用できない。又、本文書の画像スキャンしたラスターデータをそのままやりとりするため、何らかの方法でテキストデータ化しないと、本文の内容を2次利用できない等の問題点を有していた。

【0017】本発明は、前記従来の問題点を解消するべくなされたもので、紙ベースの認証システムと電子認証システムの両方で利用可能であり、電子データ化が容易で、且つ、改竄防止性能も高い認証書類を提供することを第1の課題とする。

【0018】本発明は、又、前記認証書類の作成に適した認証用紙を提供することを第2の課題とする。

【0019】本発明は、又、前記認証書類の発行方法及び装置を提供することを第3の課題とする。

【0020】本発明は、又、前記認証書類の検証方法及び装置を提供することを第4の課題とする。

【0021】

【課題を解決するための手段】本発明は、認証書類に、視覚により確認可能な認証内容、認証者情報及び認証者印影と、前記認証内容を記述した認証内容データのバーコード、及び、該認証内容データを暗号化した電子署名データのバーコードと、を共に記載することにより、前記第1の課題を解決したものである。

【0022】更に、前記認証書類に、認証機関による認証者の電子証明書データのバーコードも記載したものである。

【0023】又、前記認証内容データを、マークアップ言語で記述したものである。

【0024】又、前記電子署名データを、前記認証内容データをハッシュ化し、認証者の秘密鍵で暗号化したデータとしたものである。

【0025】又、前記バーコードを、2次元バーコードとしたものである。

【0026】又、前記データが、直接バーコード化できない場合、テキストデータに変換してからバーコード化したものである。

【0027】又、前記電子証明書データを、認証機関によって認証された、認証者の公開鍵や署名アルゴリズムとしたものである。

【0028】本発明は、又、認証用紙に、認証者情報や認証者印影、及び、認証者の電子証明書データを予め印刷することにより、前記第2の課題を解決したものである。

【0029】本発明は、又、データベースから認証内容を記述した認証内容データを呼び出す手順と、前記認証内容を記述したデータを暗号化して電子署名データを作成する手順と、各データをバーコード化する手順と、視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、及び、該認証内容データを暗号化した電子署名データのバーコードを印刷する手順とにより、認証書類を発行するようにして、前記第3の課題を解決したものである。

【0030】更に、認証機関による認証者の電子証明書データを呼び出す手順と、該電子証明書データをバーコード化する手順と、該バーコードを印刷する手順と、を含むようにしたものである。

【0031】更に、前記認証内容データをマークアップ言語化する手順を含むようにしたものである。

【0032】更に、直接バーコード化できないデータを、テキストデータに変換する手順を含むようにしたものである。

【0033】又、前記認証内容データをハッシュ化し、認証者の秘密鍵で暗号化することにより、前記電子署名データを作成するようにしたものである。

【0034】本発明は、又、認証書類の発行装置を、データベースから認証内容を記述した認証内容データを呼び出す手段と、前記認証内容を記述したデータを暗号化して電子署名データを作成する手段と、各データをバーコード化する手段と、視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、及び、該認証内容データを暗号化した電子署名データのバーコードを印刷する手段を用いて構成することにより、前記第3の課題を解決したものである。

【0035】本発明は、又、認証書類の発行装置を、データベースから認証内容を記述した認証内容データを呼び出す手段と、前記認証内容を記述したデータを暗号化して電子署名データを作成する手段と、認証機関による認証者の電子証明書データを呼び出す手段と、各データをバーコード化する手段と、視覚により確認可能な認証

内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、該認証内容データを暗号化した電子署名データのバーコード、及び、前記電子証明書データのバーコードを印刷する手段と、を用いて構成することにより、前記第3の課題を解決したものである。

【0036】本発明は、又、視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、及び、該認証内容データを暗号化した電子署名データのバーコードが共に印刷された認証書類から、バーコードを読み取る手順と、読み取った電子署名データを復号化する手順と、該復号化した電子署名データと前記認証内容データをハッシュ化したものを比較して、改ざんの有無と認証者の本人性を判定する手順とにより、認証書類を検証するようにして、前記第4の課題を解決したものである。

【0037】更に、前記認証書類に印刷されている、認証機関による認証者の電子証明書データのバーコードを読み取る手順を含むようにしたものである。

【0038】又は、事前に入手している、認証機関による認証者の電子証明書データを呼び出す手順を含むようにしたものである。

【0039】又、前記電子証明書データに含まれる認証者の公開鍵を用いて、前記電子署名データを復号化するようにしたものである。

【0040】本発明は、又、認証書類の検証装置を、視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、該認証内容データを暗号化した電子署名データのバーコード、及び、認証機関による認証者の電子証明書データのバーコードが共に印刷された認証書類から、バーコードを読み取る手段と、読み取った電子署名データを復号化する手段と、該復号化した電子署名データと前記認証内容データをハッシュ化したものを比較して、改ざんの有無を判定する手段を用いて構成することにより、前記第4の課題を解決したものである。

【0041】本発明は、又、認証書類の検証装置を、視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、及び、該認証内容データを暗号化した電子署名データのバーコードが共に印刷された認証書類から、バーコードを読み取る手段と、事前に入手している、認証機関による認証者の電子証明書データを呼び出す手段と、読み取った電子署名データを復号化する手段と、該復号化した電子署名データと前記認証内容データをハッシュ化したものを比較して、改ざんの有無及び認証者の本人性を判定する手段とを用いて構成することにより、前記第4の課題を解決したものである。

【0042】

【発明の実施の形態】以下図面を参照して、本発明の実

施形態を詳細に説明する。

【0043】今、図1に示す如く、紙ベースの認証システムで運用している部門Aと、電子認証システムで運用している部門Bと、部門Aと部門Bを電子認証している、例えば最上位に位置するルート認証局あるいは信頼できる中間認証局である上位（管理）部門C（認証機関）を想定する。

【0044】前記部門Aには、例えば、認証内容のデータベースを含むパソコン10A及び認証書類発行用のプリンタ12Aが備えられている。この部門Aには、矢印Dに示す如く、上位部門Cから当該部門Aの秘密鍵データ20Aと、当該部門Aの公開鍵を含み、上位部門Cの電子署名がされている、部門Aの電子証明書データ22Aと、上位部門Cの公開鍵を含む、部門Cの電子証明書データ（図示省略）が配布されているとする。

【0045】又、前記部門Bには、例えば、部門Aと同様のパソコン10B及びプリンタ12Bと、バーコードリーダ14とが備えられている。この部門Bには、矢印Eに示す如く、上位部門Cから、当該部門Bの秘密鍵データ20Bと、当該部門Bの公開鍵を含み、上位部門Cの電子署名がされている、部門Bの電子証明書データ22Bと、上位部門Cの公開鍵を含む、部門Cの電子証明書データ（図示省略）を配布されているとする。

【0046】まず、矢印Fに示す如く、紙ベースの認証システムの部門Aで発行した認証書類30Aを、電子認証システムの部門Bで事務処理する場合について説明する。

【0047】部門Aで認証書類30Aを発行する手順を図2に示す。

【0048】部門Aでは、認証書類の発行要求者の要望に応じて、ステップ100で認証内容32Aをデータベースから呼び出し、呼び出したデータを、必要に応じてXML等のマークアップ言語で記述すると共に、バーコードの仕様上、直接バーコード化できないバイナリデータは、例えばBase64でテキストデータに変換して、認証内容データとする。

【0049】次いでステップ102で、該認証内容データを、例えばハッシュ化してメッセージダイジェストを作成し、部門Aの秘密鍵データ20Aで暗号化して電子署名データを作成する。

【0050】次いでステップ104で、必要に応じて、部門Aの上位部門Cによる電子証明書データ22Aを呼び出す。なお、部門Aと部門Bが頻繁に認証書類をやり取りする際には、事前に部門Aと部門Bとが、上位部門Cによって認証された部門Aと部門Bの電子証明書データを交換しておくことによって、認証書類の電子証明書データを省略することもできる。この場合には、ステップ104は不要である。

【0051】次いでステップ106、108、110で、前出ステップ100、102、104で作成された

データを、それぞれ、例えば2次元バーコード化する。なお、バーコード化する順番は任意であり、特に認証書類の電子証明書データを省略した場合には、当然ステップ110も不要である。

【0052】次いでステップ112に進み、図1に符号30Aで示す如く、従来の紙の認証書類に記載されていた認証内容（ここでは文章）32A、部門Aの名称34A、部門Aの印影36Aに加えて、認証内容32Aのバーコード33A、ステップ102で作成された電子署名データのバーコード38A、及び、ステップ104で作成された電子証明書データのバーコード40Aを印刷して、紙の認証書類30Aとする。

【0053】次に、前記のようにして作成された紙の認証書類30Aは、図3に示すような手順に従って、部門Bにより検証される。

【0054】即ち、部門Bでは、まずステップ200、202、204で、紙の認証書類30Aから、例えばバーコードリーダ14（スキャナでも良い）を用いて、バーコード33A（認証内容）、バーコード38A（電子署名データ）、バーコード40A（電子証明書）を読み取る。この際、Base64でテキストデータに変換されていたバイナリデータは、Base64で逆変換してバイナリデータに戻す。又、電子証明書データのバーコードが省略されている場合には、ステップ204で、事前に入手している電子証明書データを読み出す。

【0055】次いでステップ206で、部門Cの電子証明書データを基に、例えばバーコード40Aに記述された部門Aの電子証明書データ22Aが上位部門Cで認証されていることを確認したら、該電子証明書データ22Aに含まれる部門Aの公開鍵データを取り出す。

【0056】次いでステップ208に進み、ステップ206で取り出した公開鍵を用いて、ステップ202で読み取った電子署名データを復号化し、メッセージダイジェストiを作成する。

【0057】次いでステップ210に進み、ステップ200で読み取った認証内容データをハッシュ化して、メッセージダイジェストiiを作成する。

【0058】次いでステップ212に進み、メッセージダイジェストiとiiを比較し、一致する場合には、ステップ214で、認証内容の本人認証と非改ざんを確認する。

【0059】一方、メッセージダイジェストiとiiが不一致の場合には、ステップ216に進み、認証内容の本人認証及び非改ざんを承認しない。

【0060】このようにして、認証書類の内容の電子化、認証内容の非改ざんの証明、及び認証書類の部門Aの本人証明を実現することができ、内容を確認した後、直ちに電子データを電子認証システムで扱うことが可能となる。

【0061】一方、電子認証システムの部門Bで認証し

た書類を、図1の矢印Gに示す如く、紙ベースの認証の部門Aで事務処理する場合には、部門Aの場合と同様に、部門Bでも、従来の認証内容32B、部門Bの名称34B、部門Bの印影36Bに加えて、認証内容をマークアップ言語で記述した認証内容データ、これをハッシュ化して部門Bの秘密鍵で暗号化した電子署名データ、上位部門Cによって証明されている部門Bの電子証明書データを、それぞれ例えば2次元バーコード33B、38B、40B化し、紙の認証書類30Bとして印刷する。この際、バイナリデータであって、バーコードの仕様上、直接バーコード化できない場合には、例えばBase64でテキストデータに変換してからバーコード化する。

【0062】この認証書類30Bを、部門Aでは、紙ベースであるので、従来と同様に、認証内容32B、部門名称34B、部門印36Bにより目視で内容を確認する。なお、何らかの不具合等で、部門Aから部門Bに認証書類を返送する必要がある場合には、部門Bでは、バーコードリーダ14でバーコードを読み取って、再度内容を取り込むことが可能である。

【0063】本実施形態においては、バーコードとして、2次元バーコードを用いているので、少ない面積で、多くの情報を記述できる。なお、バーコードの種類は、これに限定されない。

【0064】又、本実施形態においては、バーコードの仕様上、直接バーコード化できない場合には、Base64でテキストデータに変換してからバーコード化するようにしているので、バイナリデータであっても、バーコード化可能である。なお、バイナリデータをテキストデータに変換する方式はBase64に限定されず、例えばUNIX（登録商標）標準のuuencodeや、Macintoshで用いられているBinHexといった方式を用いることも可能である。

【0065】更に、本実施形態においては、マークアップ言語XMLのデータにしてからバーコード化しているので、項目と内容が明瞭となり、認証内容の2次利用が容易である。なお、マークアップ言語の種類はXMLに限定されず、HTML、TEX、SGML等を用いることも可能である。又、マークアップ言語化を省略することも可能である。

【0066】なお、前記実施形態においては、全ての情報をプリンタで印刷するようにしていたが、例えば図4に示す如く、認証者情報34や認証者印影36、及び、認証者の電子証明書データのバーコード40等の固定されたデータが予め印刷されている認証用紙50を用いて、印刷の負荷を軽減することも可能である。

【0067】本発明の適用対象は、地方自治体における証明書発行や登録処理に限定されず、一般の領収書発行や、会計処理等にも同様に用いることができることは明らかである。

【0068】

【発明の効果】本発明によれば、認証書類の内容の電子化、認証書類の非改ざんの証明、認証書類の認証者の本人証明を実現でき、紙ベースの認証システムと電子認証システムのどちらでも利用可能であるという優れた効果を有する。

【図面の簡単な説明】

【図1】本発明に係る認証書類の発行方法及び検証方法を実施するシステムの例の全体構成を示すブロック線図

【図2】本発明の実施形態における認証書類の発行手順を示す流れ図

【図3】同じく認証書類の検証手順を示す流れ図

【図4】同じく認証用紙の例を示す正面図

【符号の説明】

* A、B…部門

C…上位部門（認証機関）

10A、10B…パソコン

12A、12B…プリンタ

14…バーコードリーダー

20A、20B…秘密鍵データ

22A、22B…電子証明書データ

30A、30B…認証書類

32A、32B…認証内容

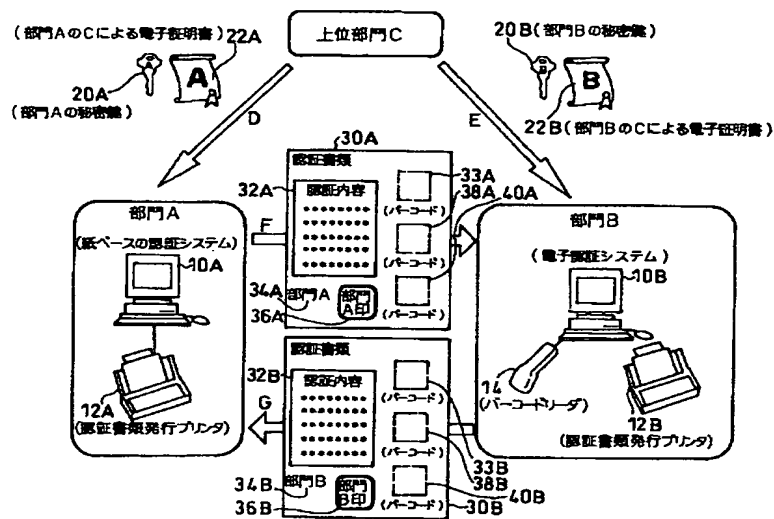
34、34A、34B…部門名称

36、36A、36B…部門印

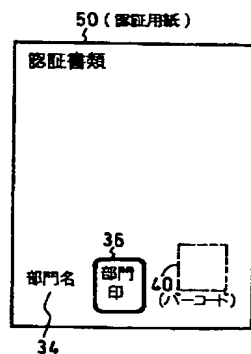
33A、33B、38A、38B、40、40A、40B…バーコード

* 50…認証用紙

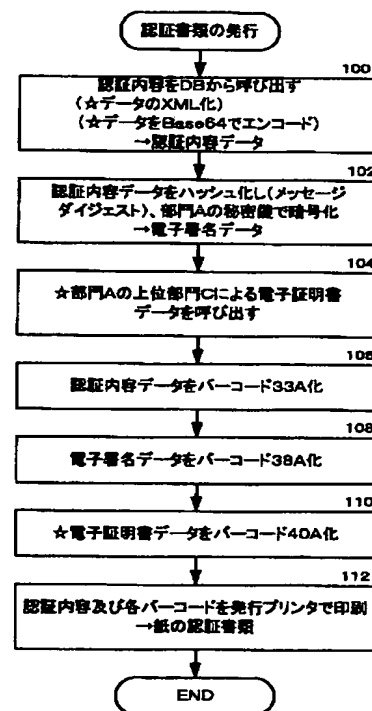
【図1】



【図4】

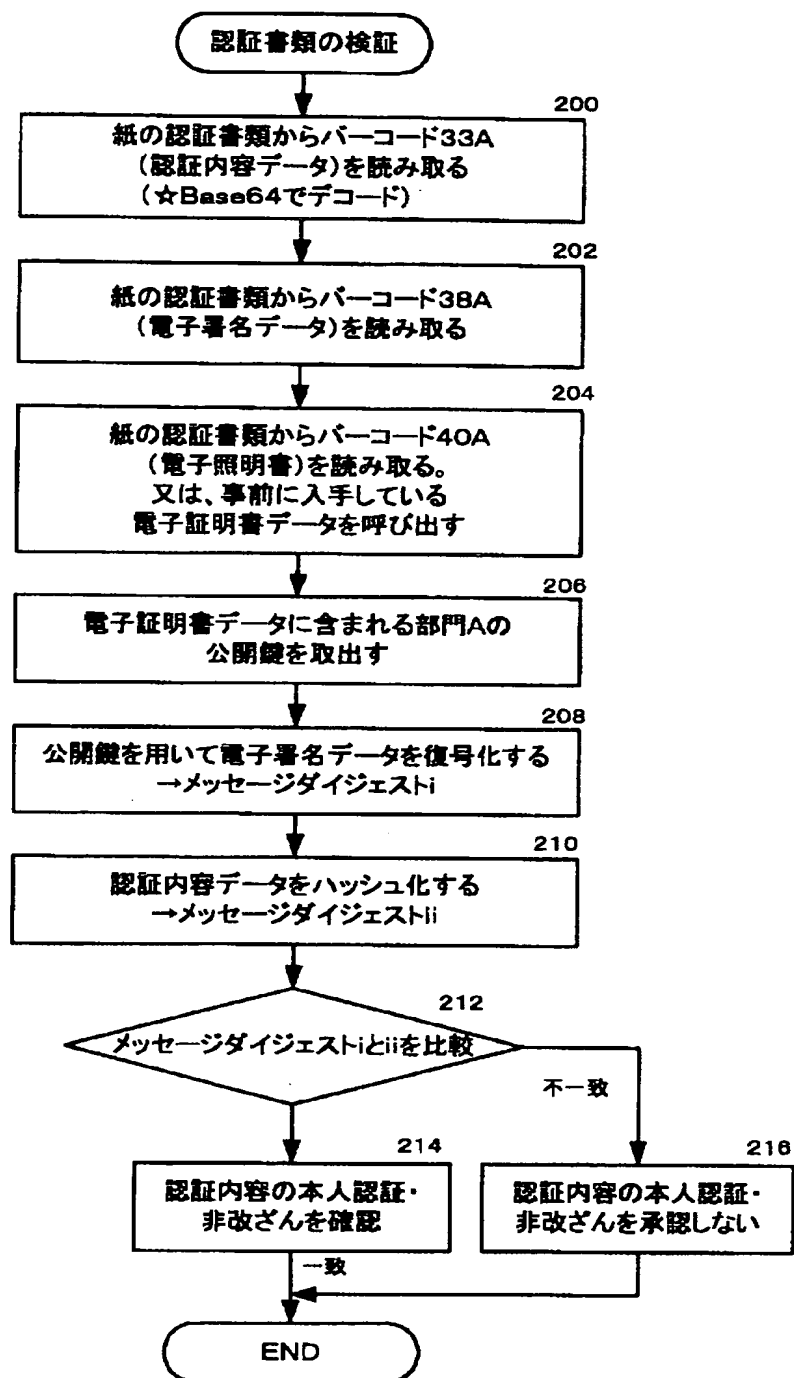


【図2】



★はオプション

【図3】



☆はオプション

フロントページの続き

(51)Int.Cl.⁷

識別記号

F I

ターマコード (参考)

G 0 6 K 19/06

G 0 7 D 7/20

G 0 7 D 7/20

G 0 6 K 19/00

A